UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MASSACHUSETTS

UNITED STATES OF AMERICA	)	
v.	)	No. 22-CR-10141
SEAN O'DONOVAN, Defendant	)	

MOTION TO SUPPRESS

Now comes the defendant Sean O'Donovan, by and through undersigned counsel, and, pursuant to Fed. R. Crim. P. 41 and the Fourth Amendment to the United States Constitution, hereby respectfully moves this Honorable Court to suppress all evidence seized pursuant to the search warrants for Mr. O'Donovan's AT&T Wireless phone records, his Apple iCloud account, and his cell phone.

This case is representative of what appears to be a regular practice in this District by which the U.S. Attorney's Office, upon developing a suspicion that a person has been involved in criminal conduct, seizes the entirety of their communications and other records stored in the "cloud" or another similar online account. These materials, which are often automatically saved from an individual's phone, are voluminous and contain a wide range of personal information. Particularly troubling is the fact that the government, in this case and others like it, simply demanded that Apple produce the entirety of the suspect's iCloud records for the specified date range. It made little attempt to narrow the universe of materials subject to the initial seizure, notwithstanding the fact that the scope of any arguable probable cause was decidedly narrow,

i.e., an alleged attempt to bribe a single Medford public official in connection with a single marijuana licensing decision. Instead, the government, again operating under what appears to be a regular practice, engaged in a seize now, narrow later approach. First, it called for Apple to produce all the documents from Mr. O'Donovan's account for the relevant date range, then it set out a series of categories of items "to be searched and seized by law enforcement." But even these purportedly narrower categories were broad enough to permit executing agents standardless discretion to search whatever they chose, in violation of the Fourth Amendment's particularity requirement.

If the foregoing were not enough, the government followed the iCloud searches by seizing the entire contents of Mr. O'Donovan's cell phone, which he used in significant part for his active law practice. The warrant for Mr. O'Donovan's cell phone included the same broad search categories as its predecessors, but was rendered even more problematic for failure to include any date limitation whatsoever.

Because no reasonable officer could have believed in the validity of a warrant that purported to authorize the search and seizure of Mr. O'Donovan's entire iCloud account or cell phone, any materials seized beyond the scope of whatever probable cause this Court determines to have existed must be suppressed. Of course, if the Court finds no probable cause, the entire fruits of the searches must be suppressed. If, alternatively, the Court finds probable cause limited to suspected bribery of the Medford Chief of Police in connection with a marijuana licensing application by Mr. O'Donovan's Client, it should suppress any materials beyond that narrow scope.

REQUEST FOR ORAL ARGUMENT

Mr. O'Donovan respectfully requests that oral argument be held on this Motion.

MEMORANDUM OF LAW

A. Background

On March 5, 2021, the government applied for a search warrant for Mr. O'Donovan's AT&T Wireless phone records. The application was based on an affidavit executed by FBI Special Agent Matthew Elio ("March Affidavit," attached hereto as Exhibit A). The affidavit asserted, at the outset of its statement of probable cause, that the FBI had "received information regarding a possible bribery attempt relating to a marijuana establishment proposed to be located in Medford, Massachusetts." Ex. A ¶ 8. The ensuing factual allegations were all based on Mr. O'Donovan's interactions with Individual 1 (referred to in the affidavit as "CHS"), which related to a single client of Mr. O'Donovan's applying for a marijuana license in Medford.

More specifically, on February 10, 2021, Mr. O'Donovan met with Individual 1, whose close relative was the Medford Chief of Police ("Chief") and member of the city's Cannabis Advisory Committee ("CAC"), and asked Individual 1 to "talk to" the Chief regarding his Client. *Id.* ¶ 13. Mr. O'Donovan went on to specifically instruct Individual 1, "Don't ask [the Chief] for any favors… just ask him to give [the Client's application] a look." *Id.* Mr. O'Donovan allegedly offered Individual 1 $25,000 for his efforts. *See id.*

After an exchange of text messages, Mr. O'Donovan and Individual 1 met again on February 22, 2021. Mr. O'Donovan explained the Medford CAC's procedure for scoring applicants. He then told Individual 1, "I wanna try to get the edge 'cause I know everybody's trying to get the edge." *Id.* ¶ 18. Mr. O'Donovan went on to opine that the Chief "has the

mayor's ear" and said, "we wanna ask [the Chief] to give [the Client] a really good shake." *Id.* Mr. O'Donovan also emphasized the strength of the Client's application, saying he "would never embarrass" Individual 1 or "waste [his own] time." *Id.* Mr. O'Donovan repeated his proposal to pay Individual 1 $25,000, or possibly as much as $50,000, for his assistance. *See id.*

In addition to recounting the interactions with Individual 1, the March Affidavit noted significant contacts between Mr. O'Donovan's phone and a phone belonging to another member of the Medford CAC, the city's Building Commissioner. *See id.* ¶¶ 19-21. There were also phone contacts between Mr. O'Donovan and the CEO of the Client, which of course was unsurprising given the attorney-client relationship. *See id.* ¶ 22.

The March Affidavit's statement of probable caused concluded with Agent Elio's opinion that "there is probable cause to believe that O'Donovan and possibly others yet unknown are engaged in a scheme to pay [Individual 1], with the corrupt intent for [Individual 1] to influence [the Chief] in connection with the marijuana application O'Donovan plans to submit for his" Medford Client. *Id.* ¶ 24. This opinion is repeated in functionally identical terms in each of the subsequent affidavits. Ex. C ¶ 28; Ex. E ¶ 49; Ex. G ¶ 36.

On March 5, 2021, Magistrate Judge Cabell issued the warrant to AT&T Wireless ("AT&T Wireless Warrant," attached hereto as Exhibit B). Attachment B to the warrant, titled "Particular Things to be Seized," called for AT&T Wireless to produce essentially all of Mr. O'Donovan's cell phone records, including the contents of all messages, for a more than two-month period from January 1, 2021 to the warrant's issuance. *See* Ex. B at 4-5. A subsequent section of Attachment B purported to set forth a (marginally) more limited category of "[i]nformation to be seized by the government," namely "[a]ll information . . . that constitutes

fruits, evidence and instrumentalities of violations of 18 U.S.C. § 666(a)(2) involving Sean O'Donovan from January 1, 2021 to the present." *Id.* at 6. The document went on to enumerate ten categories of information subject to seizure:

a. Payments to individuals made with the intent to corruptly influence Medford, Massachusetts public officials;

b. Contacts with or about public officials who have influence or authority over the licensing or approval of marijuana establishments;

c. Passwords, encryption keys, and other access devices that may be necessary to access messaging applications;

d. Contextual information necessary to understand the evidence described in this attachment;

e. Preparatory steps taken in furtherance of the bribery scheme;

f. Evidence indicating how and when the cellular device and associated cellular service was used to determine the chronological context of cellular device use, account access, and events relating to the crime under investigation;

g. Evidence indicating the geographic location of the cellular device at times relevant to the investigation;

h. Evidence indicating the cellular device owner or user's state of mind as it relates to the crime under investigation;

i. The identity of the person(s) who created the account associated with the cellular device and/or used the cellular device, including records that help reveal the whereabouts of such person(s); and

j. The identity of the person(s) who sent to and/or received communications from the cellular device about matters relating to bribery in violation of 18 U.S.C. § 666(a)(2), including records that help reveal their whereabouts.

See id. at 6-7.

On April 9, 2021, the government applied for a second search warrant, this one directed to Apple. Again, the application was supported by an affidavit executed by Agent Elio ("April Affidavit," attached hereto as Exhibit C). The affidavit repeated the same information regarding the Medford marijuana application process and Mr. O'Donovan's interactions with Individual 1 that were included in the March Affidavit. It also repeated the same information regarding Mr. O'Donovan's phone contact with the Medford Building Commissioner. The affidavit went on to represent that the information produced by AT&T Wireless pursuant to the prior warrant indicated that more messages had been sent and received by Mr. O'Donovan than AT&T Wireless had records of. *See* Ex. C ¶¶ 22-23. The records produced by AT&T Wireless also reflected Mr. O'Donovan's contacts with a Medford City Councilor who was involved in crafting the Medford CAC guidelines. *See id.* ¶¶ 24-26.

Magistrate Judge Cabell issued the warrant on April 9, 2021 ("First Apple Warrant," attached hereto as Exhibit D). The warrant, again, prescribed a two-step process. The first called for Apple to produce essentially all data from Mr. O'Donovan's iCloud account[1] from

[1] As described in Agent Elio's affidavit, "iCloud is a file hosting, storage, and sharing service provided by Apple. . . . If a user signs up for iCloud, iCloud automatically backs up information on the user's mobile devices, such as an iPhone or iPad, daily over wifi . . . , unless the user manually changes the settings to prevent automatic backups. The backup includes, among other things, purchase history from the iTunes store and App Store, photos and videos, device settings, app data, iMessage, text messages, visual voicemail password, and device settings." Ex. C ¶ 34c.

January 1, 2021 on. *See* Ex. D at 4-9. A subsequent section of the warrant attachment purported to specify "Records and Data to be Searched and Seized by Law Enforcement Personnel." *Id.* at 10. Agents were permitted to search for "[e]vidence, fruits, or instrumentalities of violations of Title 18 United States Code Sections 371 (Conspiracy) and 666 (Bribery) from January 1, 2021 to present," including documents concerning 13 specified categories. The first four categories were functionally identical to those contained in the AT&T Wireless Warrant. The category for evidence of "state of mind" was altered to refer to the owner/user of the "Target Account" rather than "cellular device," but otherwise remained the same. *Id.* The First Apple Warrant added the following categories

e. Financial accounts used to fund or receive payments related to bribery;

g. The identity of the person or persons who have owned or operated the electronic account designated in Attachment A or any associated accounts;

h. The existence and identity of any co-conspirators;

i. The travel or whereabouts of the person or persons who have owned or operated the electronic account designated in Attachment A or any associated electronic accounts;

j. The identity, location, and ownership of any computers used to access the Target Account;

k. Other email or internet accounts providing internet access or remote data storage;

l The existence or location of physical media storing electronic data, such as hard drives, CD- or DVD-ROMs, or thumb drives; and

m. The existence or location of paper print-outs of any data from any of the above.

See id.

The government applied for another search warrant directed to Apple on June 28, 2021 supported by another affidavit by Agent Elio ("June Affidavit," attached hereto as Exhibit E). The affidavit began by recounting the contents of the April Affidavit. It then went on to describe a subsequent April 26, 2021 recorded conversation between Mr. O'Donovan and Individual 1. During that meeting, Mr. O'Donovan said to Individual 1, "I guess maybe the best thing to do is just wait it out and see, make sure my guy files first of all . . . . But thank you for talking to [the Chief]. I mean, we'll see what happens." Ex. E ¶ 10. Mr. O'Donovan described the Chief as being "as straight and honest" as they come and discussed the Chief's relationship with the Mayor. *See id.* Mr. O'Donovan reiterated, "I guess what I really wanna ask is, if [the Chief] looked at my client's application and said this application sucks, then . . . he doesn't belong. But I guarantee you if [the Chief] takes a good look, he's gonna like him. And that's all I'm asking for." *Id.*; *see also id.* (suggesting that Individual 1 tell the Chief that the Client is "a great company" and all "I'm asking you to do is give him a fair share. . . . [A]ll I'm asking you is to read that application for me. . . . [I]f it sucks, don't vote for him . . . ."); *id.* ("I'm just asking that you give it a look cuz what we're afraid of . . . no one's gonna look at him."); *id.* ("[A]ll your [sic] doing is you're saying O'Donovan just asked me for a fair (UI). That'll get [the Chief] to read it."). The affidavit also discussed exchanges between Mr. O'Donovan and the City Councilor. On January 20, 2021, the City Councilor said that the Building Commissioner was "worried about" the Chief. Ex. E ¶ 17. Mr. O'Donovan allegedly responded, "Doing my best but . . ." *Id.* Weeks later, on February 12, 2021, Mr. O'Donovan texted the City Counselor that the Chief "may need to be taken to task." *Id.* ¶ 21. Mr. O'Donovan added, "The main thing is to ensure that the application & scoring complies with the ordinances codified by the city council."

Id. The affidavit additionally relayed certain conversations between Mr. O'Donovan and the Building Commissioner, some relating to the CAC process.

Magistrate Judge Cabell issued the warrant on June 28, 2021 ("Second Apple Warrant," attached hereto as Exhibit F). This warrant included only the second aspect of the prior Attachment B, namely the "Records and Data to be Searched and Seized by Law Enforcement Personnel." This was because the government sought authorization to search the same records that Apple had already produced, but extending the start of the date range for the search back to December 1, 2019. *See* Ex. E ¶ 48. The request for a broader time period was based on unspecified "phone records" reflecting "extensive communication between" Mr. O'Donovan and the City Councilor "throughout 2020," when the City Councilor was "actively involved" in the Medford marijuana licensing process. *Id.* ¶ 41.[2] The Second Apple Warrant set forth the same 13 categories reflected in the prior warrant, but granted the government's request to extend the beginning of the date range back one year and one month to December 1, 2019. *See* Ex. F at 4.

On January 7, 2022, the government applied for a final search warrant, this one to authorize the seizure and subsequent search of Mr. O'Donovan's cellphone ("January Affidavit," attached hereto as Exhibit G). The application was supported by a final affidavit from Agent Elio. The affidavit recounted many of the same allegations noted above regarding Mr. O'Donovan's meetings with Individual 1. It then went on to discuss two later recorded meetings, arranged by the government via Individual 1, in September 2021. In these later communications, Mr. O'Donovan again indicated that he merely wanted Individual 1 to speak

[2] To the extent that the phone records were Mr. O'Donovan's records produced pursuant to the AT&T Wireless Warrant or the First Apple Warrant, the search of 2020 communications clearly exceeded the scope of that warrant and would be grounds for suppression.

with the Chief about the merits of the Client's application. He texted on August 28, 2021, "Tell [the Chief] to vote [the Client] #1 as they are the best candidate for Medford legitimately." Ex. G ¶ 17. At the ensuing September 14, 2021 meeting, Mr. O'Donovan said, "if [the Chief] was gonna vote for them anyway and you're giving them a high vote that's what I'm looking for." *Id.* ¶ 18. Two weeks later, on September 29, Individual 1 requested another meeting and introduced the fiction that the Chief had originally not ranked the Client in his top three applicants, but was "gonna change the ranking" and "move them top, number one" because Individual 1 was "getting paid." *Id.* ¶ 21. Mr. O'Donovan responded, "Perfect." *Id.* After Individual 1's request for a down payment, Mr. O'Donovan provided $2,000 in cash at an October 11, 2021 meeting. *See id.* ¶ 29. The final affidavit includes no specific allegations regarding Mr. O'Donovan's interactions with the City Councilor or the Building Commissioner.

The final warrant, issued by Magistrate Judge Cabell on January 7, 2022 ("Cell Phone Warrant," attached hereto as Exhibit H), calls for seizure of the cell phone and permits off-site search for a list of 13 categories of information functionally identical to those reflected in the Apple Warrants (some categories are paraphrased to reflect the fact that the iPhone, rather than the iCloud account, is being searched). *See* Ex. H at 4-5. There is, however, no date restriction in the Cell Phone Warrant. *See id.*

B. Legal Standard

The Fourth Amendment to the United States Constitution provides that "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by

Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." U.S. Const. amend. IV.

The probable cause standard requires "more than bare suspicion." *Brinegar v. United States*, 338 U.S. 160, 175 (1949). Rather, probable cause "exists where the facts and circumstances within [the officers'] knowledge and of which they had reasonable trustworthy information [are] sufficient in themselves to warrant a man of reasonable caution in the belief that an offense has been or is being committed." *Id.* at 175-76 (citation omitted). Application of a lesser standard would "leave law-abiding citizens at the mercy of the officers' whim or caprice." *Id.* at 176. Absent exigent circumstances, the probable cause determination must be made by a "neutral and detached magistrate." *Illinois v. Gates*, 462 U.S. 213, 240 (1983) (citation omitted). And officers must present sufficient information to that magistrate to allow it to conduct the required analysis. In other words, the magistrate's "action cannot be a mere ratification of the bare conclusions of others." *Id.* at 239.

The Fourth Amendment's particularity requirement is intended to "make[] general searches . . . impossible and prevent[] the seizure of one thing under a warrant describing another. As to what is to be taken, nothing is left to the discretion of the officer executing the warrant." *Marron v. United States*, 275 U.S. 192, 196 (1927); *see also United States v. Levasseur*, 699 F. Supp. 965, 982 (D. Mass. 1988) (Young, J.), *rev'd in part on other grounds*. "Vivid in the memory of the newly independent Americans were those general warrants known as writs of assistance under which officers of the Crown had so bedeviled the colonists. . . . They were denounced by James Otis as 'the worst instrument of arbitrary power, the most destructive of English liberty, and the fundamental principles of law, that ever was found in an English law book,' because they placed

'the liberty of every man in the hands of every petty officer.'" *Stanford v. Texas*, 379 U.S. 476, 481 (1965). "[T]he problem [posed by the general warrant] is not that of intrusion *per se*, but of a general, exploratory rummaging in a person's belongings . . . ." *United States v. Fuccillo*, 808 F.2d 173, 175 (1st Cir. 1987) (quoting *Coolidge v. New Hampshire*, 403 U.S. 443, 467 (1971)). "The particularity requirement demands that a valid warrant: (1) must supply enough information to guide and control the executing agent's judgment in selecting where to search and what to seize, and (2) cannot be too broad in the sense that it includes items that should not be seized." *United States v. Kuc*, 737 F.3d 129, 133 (1st Cir. 2013).

"[T]he remedy in the case of a seizure that casts its net too broadly is" suppression of all materials "that reasonably fell outside the [legally permissible] scope of the warrant." *United States v. Aboshady*, 951 F.3d 1, 9 (1st Cir. 2020) (citation omitted); *see also United States v. Levasseur*, 704 F. Supp. 1158, 1173 (D. Mass. 1989) (Young, J.).

C. Argument

1. *The March, April, and June Affidavits, supporting the AT&T Wireless and Apple Warrants, did not give rise to probable cause that Mr. O'Donovan was involved in any bribery scheme*

Mr. O'Donovan has a pending Motion to Dismiss the Indictment in this case on the grounds that the alleged facts, which largely consist of selections from the same recorded conversations recounted in the affidavits at issue here, do not constitute bribery under either § 666 or § 1346. Mr. O'Donovan contends that, at least up until the September 29, 2021 recorded meeting, the conversations reflect nothing more than a lawful and legitimate lobbying arrangement, protected by the First Amendment, pursuant to which Mr. O'Donovan would pay Individual 1 to speak with the Chief regarding the merits of the Client's application. *See* Dkt. 19

at 15-18; *see also* Dkt 28 (Mot. to Dismiss Reply) at 11-12; Dkt. 22 (Mot. to Dismiss for Outrageous Gov't Conduct) at 7-10; Dkt. 38 (Outrageous Gov't Conduct Reply) at 3-6. The defense incorporates herein the foregoing argument from its Motion to Dismiss and other relevant pleadings.

While Mr. O'Donovan maintains that the government's alleged facts, even including those regarding September 29, do not constitute a crime, in the event this Court disagrees and therefore denies the Motion to Dismiss, the defense contends that the first three affidavits, all of which pre-dated the September 29 meeting, do not give rise to probable cause to believe that Mr. O'Donovan had committed any crime. The agent's mere speculation regarding the possibility of some criminal conduct based on the otherwise innocuous allegations does not usurp this Court's role in weighing the underlying factual content under the applicable probable cause standard. *See United States v. Ventresca*, 380 U.S. 102, 109 (1965) ("Recital of some of the underlying circumstances in the affidavit is essential if the magistrate is to perform his detached function and not serve merely as a rubber stamp for the police."); *Aguilar v. Texas*, 378 U.S. 108, 113 (1964) (stating that the magistrate "must judge for himself the persuasiveness of the facts relied on by a complaining officer to show probable cause" (citation omitted)). And, in the context of Mr. O'Donovan's protected First Amendment activity, "warrant requirements" such as probable cause must be applied "with particular exactitude." *Levasseur*, 699 F. Supp. at 987 (citation omitted).

2. *The initial production of Mr. O'Donovan's complete phone and iCloud records to the government violated the particularity requirement*

The first two warrants each purported to include two-steps: first, the vendors (AT&T Wireless and Apple) were required to produce all of Mr. O'Donovan's records for the specified

date range; then, the warrants proceeded to outline a series of purportedly narrower (but still exceedingly broad) categories of information "to be seized" or "searched and seized" by the government. The problem, of course, is that a seizure had already occurred at the first step, when the government demanded production of the full set of records. Otherwise, there would have been no need for a warrant at that stage. There can be no serious suggestion that probable cause existed for the seizure of Mr. O'Donovan's full phone records from January 1, 2021 on, or, even more problematic, the entire contents of his iCloud account going back to that same date.

This seize now, narrow later approach appears to be a regular practice by the U.S. Attorney's Office in this District. *See, e.g.*, *United States v. Kanodia*, No. 15-CR-10131, 2016 WL 3166370, at *6-7 (D. Mass. June 6, 2016). But the legal authority used to justify the procedure is far afield from the present context involving seizure of an entire iCloud account. In *United States v. Upham*, 168 F.3d 532 (1st Cir. 1999), officers executing a search warrant on the defendant's home seized his computer. The First Circuit rejected a defense argument that the warrant purporting to authorize such seizure lacked particularity because, "[a]s a practical matter, the seizure and subsequent off-premises search of the computer . . . was about the narrowest definable search and seizure reasonably likely to obtain" the suspected child pornography. *Id.* at 535.

Technology has advanced in the more than two decades since *Upham*, such that wholesale seizure of electronic evidence is sometimes far from the narrowest practical alternative. In the circumstances of this case, where Mr. O'Donovan's data was remotely accessible via his iCloud account, there was no evident reason why the government could not have constructed a narrower set of demands consistent with the scope of probable cause, which

as discussed in detail below was quite limited to the extent it existed at all. Indeed, one district court has distinguished *Upham* and other similar cases from other circuits on the grounds that they "addressed the search of computers and hard drives, not email accounts." *United States v. Matter of Search of Info. Associated With Fifteen Email Addresses Stored at Premises Owned*, No. 17-CM-3152, 2017 WL 4322826, at *6 (M.D. Ala. Sept. 28, 2017). "'[H]ard drive searches require time-consuming electronic forensic investigation with special equipment' due to the myriad ways one can hide evidence on a hard drive. 'By contrast, . . . when it comes to [online] account searches, the government need only send a request with the specific data sought and [the vendor] will respond with precisely that data.'" *Id.* (quoting *United States v. Blake*, 868 F.3d 960, 974 (11th Cir. 2017)).

On the other side of the constitutional balancing, namely the privacy implications of the search, a great deal has changed since *Upham* was decided in 1999. As the First Circuit recognized almost a decade ago, "[t]he storage capacity of today's cell phones is immense." *United States v. Wurie*, 728 F.3d 1, 8 (1st Cir. 2013). And the devices are "increasingly" used to "store personal user data in the cloud instead of on the device itself." *Id.* n.8 (citation omitted). "That information is, by and large, of a highly personal nature: photographs, videos, written and audio messages (text, email, and voicemail), contacts, calendar appointments, web searching and browsing history, purchases, and financial and medical records." *Id.* In short, "[j]ust as customs officers in the early colonies could use writs of assistance to rummage through homes and warehouses, without any showing of probable cause linked to a particular place or item sought," the government's practice of seizing entire iCloud accounts belonging to those suspected of criminal wrongdoing improperly results in "automatic access to a virtual warehouse of an

individual's most intimate communications and photographs without probable cause" tied to those specific materials. *Id.* at 9 (citation omitted); *see also United States v. Lofstead*, 574 F. Supp. 3d 831, 839 (D. Nev. 2021) ("District courts nationwide have begun expressing concerns about over-searching ESI, especially because warrants often authorize the government to seize large quantities of personal information that it lacks probable cause to search."). This runs afoul of the Supreme Court's command to "assur[e] preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted." *United States v. Jones*, 565 U.S. 400, 406 (2012) (citation omitted).[3]

3. *The enumerated categories of materials to be searched and seized by investigators in all four warrants exceeded the scope of any probable cause and therefore violated the particularity requirement*

Even assuming, contrary to the foregoing, that the particularity requirement does not apply to the initial seizures of Mr. O'Donovan's entire phone records and iCloud account, the categories of materials subject to search listed in all four warrants were "so numerous and unspecific to create an [effectively] unrestricted dragnet search." *Lofstead*, 574 F. Supp. 3d at 844 (citation omitted). At best, assuming there was probable cause to believe any crime had been committed, the scope of such probable cause was limited to suspected bribery of one particular Medford CAC member. But the scope of the searches purportedly permitted by the warrants was much broader, extending both to (a) "[p]ayments to individuals made with the

[3] The defense acknowledges that, in *United States v. Aboshady*, 951 F.3d 1 (1st Cir. 2020), the First Circuit affirmed the defendant's convictions in a case involving execution of a two-step warrant requiring Google to produce all of the data from the defendant's account. But the defendant in that case argued only that the government's retention of the full set of data violated the terms of the warrant itself. *See id.* at 5. The *Aboshady* Court had no occasion to consider whether the initial seizure from Google violated the Fourth Amendment particularity requirement.

intent to corruptly influence Medford, Massachusetts public officials," without any limitation to cannabis licensing; and (b) "[c]ontacts with or about" any "public officials" with no specification as to any particular state or municipality, "who have influence or authority over the licensing or approval of marijuana establishments." Ex. B at 6; Ex. D at 10; Ex. F at 4; Ex. H at 4. In short, one instance of suspected bribery by Mr. O'Donovan was insufficient to create "probable cause of ongoing or serial criminal incidents." *Lofstead*, 574 F. Supp. 3d at 840-41. The government, therefore, should not have been permitted to leverage an isolated incident of suspected bribery of a single Medford CAC member into a wide-ranging search for evidence of any other unspecified misconduct that Mr. O'Donovan may have engaged in with other public officials. The category encompassing "[f]inancial accounts used to fund or receive payments related to bribery" is similarly unlimited to the specific instance of suspected bribery at issue, and would improperly permit blanket access to any and all records of the account(s) implicated. Ex. D at 10; Ex. F at 4; Ex. H at 4.

Other of the itemized categories are so vague that they provided no meaningful guidance to investigators attempting to distinguish responsive from non-responsive materials. For example, all four warrants called for search of evidence regarding the account or device user's "state of mind as it relates to the crime under investigation." Ex. B at 6; Ex. D at 10; Ex. F at 4; Ex. H at 4. This Court has invalidated a similar category purporting to authorize seizure of documents "tending to show motive and intent." *Levasseur*, 699 F. Supp. at 982. The "state of mind" category, much like the "motive and intent" analogue, simply left "too much" to the "discretion of the executing agents" in determining which materials were subject to review. *Id.*; *see also United States v. Scanzani*, 392 F. Supp. 3d 210, 223 (D. Mass. 2019) (finding "use of

the term 'state of mind' evidence" in warrant to be "troubling" and observing, "it is far from clear whether the term is sufficiently specific to provide appropriate guidance to the executing agents"). The category for "[c]ontextual information necessary to understand the evidence" provides perhaps even more unbridled discretion, and could conceivably permit officers to review any and all documents they chose. Ex. B at 6; Ex. D at 10; Ex. F at 4; Ex. H at 4.

Agents' execution of the iCloud searches reinforces the overbreadth of the warrants. *See Levasseur*, 699 F. Supp. at 982 ("[S]trong evidence that the warrants were lacking in particularity is provided by the materials actually seized which suggest that the executing agents engaged in a general rummaging."). The government produced in discovery almost 500 pages appearing to have been extracted from Mr. O'Donovan's iCloud account, containing his messages with several individuals who have no apparent connection to the alleged Medford bribery scheme, including the former Mayor of Somerville who had no apparent relationship to Medford.

The Cell Phone warrant is rendered even more problematic than its predecessors due to the omission of any date range limiting the scope of materials to be searched. This omission is especially noteworthy in light of the fact that the supporting affidavit alleged no conduct by Mr. O'Donovan pre-dating February 2021. *See* Ex. G ¶ 7. In these circumstances, the lack of any date limitation, in and of itself, renders the Cell Phone Warrant overbroad. *See United States v. Abrams*, 615 F.2d 541, 545 (1st Cir. 1980) ("A time frame should also have been incorporated into the warrant."); *United States v. Abboud*, 438 F.3d 554, 576 (6th Cir. 2006) ("Failure to limit broad descriptive terms by relevant dates, when such dates are available to the police, will render a warrant overbroad." (citation omitted)); *United States v. Kow*, 58 F.3d 423, 427 (9th Cir. 1995)

(finding warrant insufficiently particular where "[t]he government did not limit the scope of the seizure to a time frame within which the suspected criminal activity took place"); *Lofstead*, 574 F. Supp. 3d at 843 ("[T]here is no justification for an unrestricted search without any temporal limitations here.").

4. *The good-faith exception to the exclusionary rule does not apply*

The Court should reject any claim by the government that the good-faith exception to the Fourth Amendment's general exclusionary rule should apply here. The Supreme Court has made clear that, in order for the exception to apply, "the officer's reliance on the magistrate's probable-cause determination and on the technical sufficiency of the warrant . . . must be objectively reasonable." *United States v. Leon*, 468 U.S. 897, 922 (1984). "[A] warrant may be so facially deficient—i.e., in failing to particularize the place to be searched or the things to be seized—that the executing officers cannot reasonably presume it to be valid." *Id.* at 923.

In the present case, the warrants at issue, essentially purporting to authorize seizure of Mr. O'Donovan's entire phone records, iCloud account contents, and finally his cell phone, were so facially lacking in particularity that "no officer could have reasonably presumed" they were valid. *Levasseur*, 699 F. Supp. 965 at 982; *see also, e.g.*, *Fuccillo*, 808 F.2d at 178. "The defect arises not from a lack of compliance with the Warrant[s'] terms, but from the failure of executing officers to recognize that the Warrant[s] authorize[d] a general search of [Mr. O'Donovan's] phone" and other information. *Lofstead*, 574 F. Supp. 3d at 846. "When faced with a warrant that authorizes an unrestricted search of almost all, if not explicitly all, content on a cell phone, an executing officer behaving in good faith should know that such a search is objectively unreasonable and would likely violate the defendant's Fourth Amendment rights." *Id.*

D. Conclusion

For the foregoing reasons, the defense respectfully requests that this Honorable Court suppress all evidence seized pursuant to the search warrants for Mr. O'Donovan's AT&T Wireless phone records, his Apple iCloud account, and his cell phone.

COMPLIANCE WITH LOCAL RULE 7.1(a)(2)

Undersigned counsel conferred with the Government, and the Government opposes the relief requested in this Motion.

Respectfully Submitted,
SEAN O'DONOVAN
By His Attorney,

/s/ Martin G. Weinberg
Martin G. Weinberg, Esq.
Mass. Bar No. 519480
20 Park Plaza, Suite 1000
Boston, MA 02116
(617) 227-3700
owlmgw@att.net

Dated: October 19, 2022

CERTIFICATE OF SERVICE

I, Martin G. Weinberg, hereby certify that on this date, October 19, 2022, a copy of the foregoing document has been served via Electronic Court Filing system on all registered participants.

/s/ Martin G. Weinberg
Martin G. Weinberg, Esq.